ELSEVIER

Discrete Applied Mathematics 91 (1999) 243–249

DISCRETE APPLIED MATHEMATICS

Induced permutation automata and coverings of strongly connected automata

Kenji Uemura [a], Takeo Yaku [b], Kimio Sugita [c,*]

[a] *Tsuru University, Tsuru City, 402 Japan*

[b] *Department of Applied Mathematics, College of Humanities and Sciences, Nihon University, Setagaya, Tokyo, 156 Japan*

[c] *Department of Mathematics, School of Science, Tokai University, Hiratsuka City, 259-12 Japan*

Received 18 March 1997; received in revised form 25 February 1998; accepted 31 August 1998

Abstract

Let $A=(S,\Sigma,N)$ be a strongly connected automaton and e be a minimal idempotent of characteristic semigroup $\mathscr{C}(A)$. The unique (up to isomorphism) subgroup $e\mathscr{C}(A)e$ is a very important group in automaton automorphism theory. For example, the automorphism group $\mathscr{A}(A)$ of A is a homomorphic image of a subgroup of $e\mathscr{C}(A)e$ [7, 8]. If H is a subgroup of $\mathscr{A}(A)$, then the automorphism group of the factor automaton A/H is also homomorphic to a subgroup of $e\mathscr{C}(A)e$. In this paper we show another property of $e\mathscr{C}(A)e$. First, we introduce the induced permutation automaton whose characteristic semigroup is isomorphic to $e\mathscr{C}(A)e$, and the generalized factor automaton. Using these two automata, we construct a cascade product covering of A, if $e\mathscr{C}(A)e$ is not {id} (identity permutation group). This is an example of an effective admissible subset system covering [3], as well as a generalization of the result of Krohn et al. [6] which gave a decomposition of A, if the automorphism group of A is not {id}. © 1999 Published by Elsevier Science B.V. All rights reserved.

Keywords: Algebraic automata; Automaton automorphisms; Automaton decomposition; 20B35; 20M35; 68Q70

1. Introduction

Decomposition theory of finite automata is one of the important fields in algebraic automata theory. It is concerned in covering finite automata with some kinds of products of algebraically simpler automata. The first major result in the algebraic decomposition theory was due to Krohn and Rhodes [5]. It states that any automaton is covered by a cascade product of simple-group automata and two-state reset automata. Since then many versions of this have appeared.

* Corresponding author. E-mail: sugita@sm.u-tokai.ac.jp.

PII: S0166-218X(98)00150-4

If the automorphism group of an automaton is not {id}, then it induces a factor automaton and we get a cascade decomposition of the automaton [6]. There are many results about automorphism groups of finite automata. Weeg [10] showed that the automorphism group of a strongly connected automaton is a regular permutation group on the state set. Bavel [1] studied the relation between the structure and functions of automata by introducing a primary automaton. Fleck [2] showed that the automorphism group of factor automaton A/H has a subgroup isomorphic to $\mathscr{A}(A)/H$, where H is a normal subgroup of $\mathscr{A}(A)$. Using wreath product, Uemura [9] showed its inverse. Using a permutation group $e\mathscr{G}(A)e$, Perrin et Perrot [7] and Uemura [8] characterized the automorphism group of strongly connected automaton. One problem is that the class of strongly connected automata whose automorphism group is not {id} is small.

In this paper, we introduce the notion of the induced permutation automaton of finite automaton. This idea comes from the group $e\mathscr{G}(A)e$ stated in the papers of Perrin et Perrot [7] and Uemura [8]. We also introduce the generalized factor automaton. Using these automata, we make a covering of automata. This covering is valid for the class of strongly connected automata where $e\mathscr{G}(A)e$ is not {id} which is larger than the class where $\mathscr{A}(A)$ is not {id}. This covering is valid for a larger class of strongly connected automata than the class where $\mathscr{A}(A)$ is not {id}, and is an example of an effective cascade product covering using an admissible subset system. We also mention that the automorphism group of the generalized factor automaton is {id}.

2. Previous results and definitions

This section lists some previous results and necessary definitions in algebraic automata theory. For more details, the reader might refer to item [3] in the reference section.

Definition 1. A triple $A=(S,\Sigma,N)$ is called a (finite) automaton, where S is a finite non-empty set of states, Σ is a finite non-empty set of symbols and N is a transition mapping from $S\times\Sigma$ into S. Consequently, this automaton has no initial or final states. The domain of N can be extended to $S\times\Sigma^*$, so that it satisfies $N(s,xy)=N(N(s,x),y)$ for all $x,y\in\Sigma^*$ and $s\in S$. For a subset $A\subseteq S$ and $\sigma\in\Sigma$, define $N(A,\sigma)=\bigcup_{s\in A}N(s,\sigma)$.

Let G be a finite group and define an automaton $A=(G,G,N)$ where $N(g,g_1)=gg_1$. This automaton is called a *group automaton*. An automaton is called a *permutation automaton*, if every transition mapping is a permutation on the state set. An automaton is *strongly connected*, if for any two states s and t, there is an $x\in\Sigma^*$ such that $t=N(s,x)$.

Definition 2. A permutation g on the state set S of automaton A is called an automorphism if, for any state s and for any input symbol σ, $N(s,\sigma)g=N(sg,\sigma)$. The set of

all automorphisms forms a permutation group on S, denoted by $\mathscr{A}(A)$ and called the automorphism group of A.

Definition 3. A permutation g on a finite set S is a regular permutation if there exist $s \in S$ and a positive number n such that $sg^n = s$, then g^n is the identity permutation on S. A regular permutation group is a permutation group all of whose elements are regular permutations.

It is easily shown (cf. [10]) that if an automaton A is strongly connected, then $\mathscr{A}(A)$ is a regular permutation group on S.

Definition 4. Let G be a permutation group on a set S and define a relation on S by $s \sim t$ if there exists a $g \in G$ such that $s = tg$. Then this relation is an equivalence relation. The class of the partition on S induced by this relation is called the transitivity class of G. If there is only one transitivity class of G, then G is called a transitive permutation group.

Definition 5. Let $A = (S, \Sigma, N)$ be an automaton. The relation $\sim$ on Σ^* defined by "$x \sim y \Leftrightarrow N(s,x) = N(s,y)$ for any $s \in S$" is an equivalence relation and induces a mapping semigroup on S. This semigroup is called the characteristic semigroup of automaton A and is denoted by $\mathscr{C}(A)$.

Definition 6. Let $A = (S, \Sigma, N)$ be an automaton and $\pi = \{H_i\}_{i \in I}$ be a partition on S, such that for any H_i and $\sigma \in \Sigma$, $N(H_i, \sigma) \subseteq H_j$ for some H_j. This partition is called an admissible partition.

For an automaton $A = (S, \Sigma, N)$ and an admissible partition $\pi = \{H_i\}_{i \in I}$, we can define an automaton $(\pi, \Sigma, \bar{N})$, where $\bar{N}(H_i, \sigma) = H_j$ if $N(H_i, \sigma) \subseteq H_j$ for any $H_i \in \pi$ and $\sigma \in \Sigma$. This automaton is called the *factor automaton of A with respect to π* and is denoted by A/π. Let H be a subgroup of the automorphism group of A. Consider the partition $S/H = \{s_1H, s_2H, \ldots, s_mH\}$, where $S = s_1H \cup s_2H \cup \cdots \cup s_mH$, $s_iH \cap s_jH = \emptyset$ $(i \neq j)$. Since $N(s_iH, \sigma) = N(s_i, \sigma)H$, this partition is admissible. This is defined as the *automorphism factor automaton with respect to H* and denoted by $A/H = (S/H, \Sigma, \bar{N})$.

Definition 7. Two automata $A = (S_1, \Sigma_1, N_1)$ and $B = (S_2, \Sigma_2, N_2)$ are isomorphic if there are two one-to-one correspondences $\phi : S_1 \to S_2$ and $\psi : \Sigma_1 \to \Sigma_2$ such that $N_1(s_1, \sigma_1)\phi = N_2(s_1\phi, \sigma_1\psi)$ for any $s_1 \in S_1$ and $\sigma_1 \in \Sigma_1$.

Two automata $A = (S_1, \Sigma_1, N_1)$ and $B = (S_2, \Sigma_2, N_2)$ are equivalent if there is a one-to-one correspondence $\phi : S_1 \to S_2$ and an isomorphism ψ' between $\mathscr{C}(A)$ and $\mathscr{C}(B)$ such that $(s_1x)\phi = (s_1\phi)(x\psi')$ for any $s_1 \in S_1$ and $x \in \mathscr{C}(A)$. If two automata are equivalent, then their automorphism groups are isomorphic, since their characteristic semigroups are isomorphic as mapping semigroups.

Proposition 8 (Cayley's Theorem) (Huppert [4]). *Let G be a finite group. Let $G_R = \{g_R \mid g \in G\}$ and $G_L = \{g_L \mid g \in G\}$, where $g_i g_R = g_i g$ and $g_i g_L = g g_i$. Then these are two permutation groups on G which are isomorphic to G, and their isomorphisms are $g \mapsto g_R$ and $g \mapsto g_L^{-1}$. Also $g_R g'_L = g'_L g_R$ holds for any g_R and g'_L.*

This Proposition has a very important meaning. It means that for a transitive regular finite permutation group, there is an isomorphic transitive regular permutation group on the same set (cf. [8]). And for an automaton A, there are two isomorphic permutation groups on $s\mathscr{A}(A)$, which are commutative to each other. One is a restriction of $\mathscr{A}(A)$ and the other one is a homomorphic image of a subgroup of $\mathscr{C}(A)$.

Definition 9. Let $A = (S_1, \Sigma, N_1)$ and $B = (S_2, \Sigma, N_2)$ be automata and $\phi : S_1 \to S_2$ be a surjective function, such that $N_1(s_1, \sigma)\phi = N_2(s_1\phi, \sigma)$ for any $\sigma \in \Sigma$ and $s_1 \in S_1$. Then we say A covers B and ϕ is a covering of B with A.

Definition 10. Let $A = (S_1, \Sigma_1, N_1)$ and $B = (S_2, \Sigma_2, N_2)$ be automata and $\omega : S_2 \times \Sigma_2 \to \Sigma_1$ be a function. The cascade product of A and B with respect to ω is defined by $A\omega B = (S_1 \times S_2, \Sigma_2, N)$, where $N((s_1, s_2), \sigma_2) = (N_1(s_1, \omega(s_2, \sigma_2)), N_2(s_2, \sigma_2))$ for $\sigma_2 \in \Sigma_2$, $(s_1, s_2) \in S_1 \times S_2$.

Definition 11. Let S be a semigroup. $e \in S$ is called an idempotent if $e^2 = e$. E denotes the set of idempotents of S.

Definition 12. Define a partial order on E by $e_1 \leqslant e_2 \Leftrightarrow e_1 e_2 = e_2 e_1 = e_1$. A minimal element of E is called a minimal idempotent. E_0 denotes the set of minimal idempotents.

Lemma 13 (Uemura [8]). *Let S be a finite semigroup and e_1, e_2 be its minimal idempotents. Then there exist positive integers m, n such that $(e_1 e_2 e_1)^m = e_1$, $(e_2 e_1 e_2)^n = e_2$. If m, n are the least positive integers satisfying the above conditions, then $m = n$.*

Lemma 14 (Uemura [8]). *Let S be a mapping semigroup on a finite set X, and let e_1 be a minimal idempotent and e_2 be an idempotent. Then e_2 is minimal if and only if $\#Xe_1 = \#Xe_2$.*

Theorem 15 (Uemura [8]). *Let S be a finite mapping semigroup on a finite set X and e_1, e_2 be its minimal idempotents. Then the restriction of $e_1 S e_1$ to Xe_1 is a permutation group on Xe_1. Let n be such a least integer defined in Lemma 13. Then $\phi : e_1 S e_1 \to e_2 S e_2$ defined by $(e_1 s e_1)\phi = (e_2 e_1)^n e_1 s e_1 (e_1 e_2) = (e_2 e_1)^n s e_1 e_2$ and $\psi : Xe_1 \to Xe_2$ defined by $(xe_1)\psi = xe_1 e_2$ give an isomorphism as permutation groups.*

Lemma 16. *Let $A = (G, G, N)$ be a group automaton, where $N(g, g_1) = gg_1$. Let $B = (G, G, N')$ be a automaton, such that $N'(g, g_1) = g_1^{-1} g$. With the Proposition, it is shown that A and B are isomorphic under the following correspondences $\phi : G \to G$, $(g)\phi = g^{-1}$, $\psi : G \to G$, $(g)\psi = g$.*

3. Induced permutation automaton and covering

In this section, we introduce the notion of the induced permutation automaton which induces a generalized factor automaton. With the cascade product of these two automata, we will make a covering of the original automaton. Also, we will mention that the automorphism group of the generalized factor automaton in this case is $\{\mathrm{id}\}$ and the automorphism group of A is isomorphic to a subgroup of that of the induced permutation automaton.

The following is a machine version of the theorem due to Krohn et al. [6], about semigroup decomposition.

Theorem 17. *Let $A=(S,\Sigma,M)$ be a strongly connected automaton. Then A is decomposed to a cascade product $C=(\mathscr{A}(A)\times S/\mathscr{A}(A),\Sigma,L)$ of a group automaton B which is isomorphic to the automorphism group automaton $(\mathscr{A}(A),\mathscr{A}(A),N)$ and the factor automaton $A/\mathscr{A}(A)$.*

Proof. Let $B=(\mathscr{A}(A),\mathscr{A}(A),N')$, where $N'(g,g_1)=g_1^{-1}g$ for any $g,g_1\in\mathscr{A}(A)$, and $A/\mathscr{A}(A)=(S/\mathscr{A}(A),\Sigma,\bar{N})$. Let $K=\{s_1,s_2,\ldots,s_n\}$ be a representative of $S/\mathscr{A}(A)$. Then $S=s_1\mathscr{A}(A)\cup s_2\mathscr{A}(A)\cup\cdots\cup s_n\mathscr{A}(A)$, $s_i\mathscr{A}(A)\cap s_j\mathscr{A}(A)=\emptyset$ $(i\neq j)$ and $s\in S$ is uniquely represented by (g,s_i), where $g\in\mathscr{A}(A)$, $s_i\in K$. For $s_i\in K$, $\sigma\in\Sigma$, put $M(s_i,\sigma)=s_jg$, and define a mapping ω from $S/\mathscr{A}(A)\times\Sigma$ to $\mathscr{A}(A)$ by $(s_i\mathscr{A}(A),\sigma)\omega=g^{-1}$. Then we get the relation $L((h,s_i\mathscr{A}(A)),\sigma)=(N'(h,(s_i\mathscr{A}(A),\sigma)\omega),\bar{M}(s_i\mathscr{A}(A),\sigma))=(N'(h,g^{-1}),\bar{M}(s_i\mathscr{A}(A),\sigma))=(gh,s_j\mathscr{A}(A))$. Define a mapping ϕ from $\mathscr{A}(A)\times S/\mathscr{A}(A)$ to S, by $(h,s_i\mathscr{A}(A))\phi=s_ih$, then $(\phi,\mathrm{id}_\Sigma)$ is a isomorphism from C to A. □

The class of strongly connected automata whose automorphism group is not $\{\mathrm{id}\}$ is small. To generalize this theorem, we need some more definitions, and we use covering instead of decomposition.

Let e be a minimal idempotent of $\mathscr{C}(A)$. By Theorem 15, the restriction of $e\mathscr{C}(A)e$ on Se is a permutation group. The structure of the group does not depend on e, since for different e's, they are isomorphic as permutation groups. We define a permutation automaton $(Se,e\mathscr{C}(A)e,M)$, where $M(se,exe)=sexe$, and call this automaton the *induced permutation automaton of A*.

Definition 18. Let $A=(S,\Sigma,N)$ be an automaton and $\pi=\{H_i\}_{i\in I}$ be a collection of subsets of S such that $S=\bigcup_{i\in I}H_i$ and for any H_i and $\sigma\in\Sigma$, $N(H_i,\sigma)\subseteq H_j$ for some H_j. This π is called an admissible subset system for S (or of A).

Lemma 19. *Let $A=(S,\Sigma,N)$ be a strongly connected automaton. Then $\{Se\}_{e\in E_0}$ is an admissible subset system where E_0 is the set of minimal idempotents of $\mathscr{C}(A)$.*

Proof. Let $s\in S$ and $e\in E_0$. Since A is strongly connected, $s(et)=s$ for some $t\in\mathscr{C}(A)$. Let $(et)^n$ be an idempotent and e' be a minimal idempotent such that $e'\leqslant(et)^n$. Then by

Lemma 14, $Se' \subseteq S(et)^n$. And $S(et)^n = S(et)^{n-1}(et) \subseteq S(et)$. Then $\#S(et)^n \leqslant \#S(et) \leqslant \#Se$. So $\#Se' \leqslant \#S(et)^n \leqslant \#Se$. By Lemma 14, $(et)^n$ is a minimal idempotent which satisfies the condition $s(et)^n = s$. Then for any element s, there is a minimal idempotent e which satisfies $se = s$. It is also shown with ease that for minimal idempotent e and $a \in \mathscr{C}(A)$, $(Se)a = Se'$ for some minimal idempotent e'. Then $\{Se\}_{e \in E_0}$ is an admissible subset system. □

We call the admissible subset system in Lemma 19 the *elemental admissible subset system of A*. In general admissible subset systems, $N(H_i, \sigma)$ may be contained by more than one H_j's. However, in the elemental admissible subset system, $N(H_i, \sigma)$ is contained by only one H_j.

Let $A = (S, \Sigma, N)$ be a strongly connected automaton and $\pi = \{Se\}_{e \in E_0}$ be the elemental admissible subset system of A. Then we can construct an automaton $A/\pi = (\pi, \Sigma, \bar{N})$ where $\bar{N}(Se, \sigma) = N(Se, \sigma)$. We call this automaton the *generalized factor automaton for the elemental admissible subset system*. Take an $x \in \Sigma^*$ whose transition induces a minimal idempotent e_1 of $\mathscr{C}(A)$. Then $\bar{N}(Se, x) = See_1 = Se_1$ for any $Se \in \pi$. This means that $\mathscr{A}(A/\pi) = \{\mathrm{id}\}$.

Now we are ready to state the main theorem.

Theorem 20. *Let $A = (S, \Sigma, N)$ be a strongly connected automaton. Then A is covered by a cascade product $B\omega(A/\pi) = (Se \times \pi, \Sigma, L)$ of the induced permutation automaton $B = (Se, e\mathscr{C}(A)e, M)$ and the generalized factor automaton for the elemental admissible subset system $A/\pi = (\pi, \Sigma, \bar{N})$ where e is a minimal idempotent of $\mathscr{C}(A)$.*

Proof. Let $\pi = \{Se_1, Se_2, \ldots, Se_n\}$, $Se_i \neq Se_j$ $(i \neq j)$ and $\{e_1, e_2, \ldots, e_n\} \subseteq E_0$ where $e_1 = e$. For $Se_i \in \pi$ and $\sigma \in \Sigma$, put $N(Se_i, \sigma) = Se_j$. Let $(e_j e_1 e_j)^m = e_j$ $(m \geqslant 1)$. We note $\eta_\sigma \in \mathscr{C}(A)$ as the induced element from $\sigma \in \Sigma$ (i.e. $s\eta_\sigma = N(s, \sigma)$ for any $s \in S$), and put $g_\sigma = \eta_\sigma(e_j e_1 e_j)^{m-1}$ (if $m \geqslant 2$) or $g_\sigma = \eta_\sigma$ (if $m = 1$). By Lemma 14, $(Se_1)e_i = Se_i$ and $(Se_1)e_i e_j = Se_j$. So, an element in Se_i (resp. Se_j) is represented uniquely as $se_1 e_i$ (resp. $te_1 e_i e_j$) with some $s, t \in S$. Consequently, the relation $N(Se_i, \sigma) = Se_j$ is replaced with the relation $N(se_1 e_i, \sigma) = te_1 e_i e_j$, and we get the relation $se_1 e_i g_\sigma e_1 e_j = te_1 e_i e_j$. Now, define a mapping ω from $\pi \times \Sigma$ to $e_1 \mathscr{C}(A) e_1$ by $(Se_i, \sigma)\omega = e_1 e_i g_\sigma e_1$, and a mapping ϕ from $Se_1 \times \pi$ to S by $(se_1, Se_i)\phi = se_1 e_i$. Then $L((se_1, Se_i), \sigma)\phi = (M(se_1, (Se_i, \sigma)\omega), \bar{N}(Se_i, \sigma))\phi = (M(se_1, e_1 e_i g_\sigma e_1), N(Se_i, \sigma))\phi = (se_1 e_i g_\sigma e_1, Se_j)\phi = se_1 e_i g_\sigma e_1 e_j = te_1 e_i e_j = N(se_1 e_i, \sigma) = N((se_1, Se_i)\phi, \sigma)$. Therefore, there is a covering from $B\omega(A/\pi)$ to A with ϕ. □

4. Conclusion

In this paper, we have discussed the covering of automata, and have introduced another property of $e\mathscr{C}(A)e$. We have constructed a covering of A using a cascade product of permutation automaton and a generalized factor automaton, if $e\mathscr{C}(A)e$ is

not {id}. This is a generalization of the cascade product decomposition of A, which is obtained when $\mathscr{A}(A)$ is not {id}. The transition of the elemental admissible subset system used here is uniquely determined, and this property does not hold in a general admissible subset system. Some structures of permutation automata are simple, but those of elemental admissible subset systems are not so simple. In the next step, therefore, we need to simplify the elemental admissible part of our covering.

References

[1] Z. Bavel, Structure and transition-preserving function of finite automata, J. ACM 15 (1968) 135–158.
[2] A.C. Fleck, Isomorphism group of automata, J. ACM 9 (1962) 469–476.
[3] W.M.L. Holcombe, Algebraic Automata Theory, Cambridge University Press, Cambridge, 1982.
[4] B. Huppert, Endliche Gruppen I, Springer, Berlin, 1967.
[5] K. Krohn, J.L. Rhodes, Algebraic theory of machines I: Prime decomposition theorem for finite semigroups and machines, Trans. Amer. Math. Soc. 116 (1965) 450–464.
[6] K. Krohn, R. Langer, J.L. Rhodes, Algebraic principles for the analysis of a biochemical system, J. CSS 1 (1967) 119–136.
[7] D. Perrin, J.F. Perrot, Congruences et automorphismes des automates finis, Acta Informatica 1 (1971) 159–172.
[8] K. Uemura, Semigroups and automorphism groups of strongly connected automata, M.S.T. 8 (1974) 8–14.
[9] K. Uemura, On the automorphism group of a factor automaton of a strongly connected automaton, Congr. Numer. 108 (1995) 153–159.
[10] G.P. Weeg, The structure of an automaton and its operation-preserving transformation group, J. ACM 9 (1962) 345–349.